VIII kadencja

KANCELARIA SEJMU
Biuro Komisji Sejmowych

PEŁNY ZAPIS PRZEBIEGU POSIEDZENIA

■ **Komisji Obrony Narodowej**
(nr 40)
z dnia 3 listopada 2016 r.

Pełny zapis przebiegu posiedzenia

Komisja Obrony Narodowej (nr 40)

3 listopada 2016 r.

Komisja Obrony Narodowej, obradująca pod przewodnictwem posła **Michała Jacha (PiS)**, przewodniczącego Komisji, zrealizowała następujący porządek dzienny:

– informacja Ministra Obrony Narodowej na temat bezpieczeństwa teleinformatycznego Sił Zbrojnych RP,

– informacja Ministra Obrony Narodowej na temat systemu ochrony myśli technologicznej i technologii innowacyjnych na potrzeby pozyskiwanego sprzętu wojskowego dla Sił Zbrojnych RP,

– sprawy bieżące.

W posiedzeniu udział wzięli: **Bartosz Kownacki** sekretarz stanu w Ministerstwie Obrony Narodowej wraz ze współpracownikami.

W posiedzeniu udział wzięli pracownicy Kancelarii Sejmu: **Michał Madaj**, **Kamil Strzępek**, **Jacek Zientarski** – z sekretariatu Komisji w Biurze Komisji Sejmowych.

Przewodniczący poseł Michał Jach (PiS):

Dzień dobry państwu. Witam państwa na kolejnym posiedzeniu Komisji Obrony Narodowej.

Porządek dzienny dzisiejszego posiedzenia obejmuje informację ministra obrony narodowej na temat bezpieczeństwa teleinformatycznego w Siłach Zbrojnych Rzeczypospolitej Polskiej, w pkt 2 informację ministra obrony narodowej na temat systemu ochrony myśli technologicznej i technologii innowacyjnych na potrzeby pozyskiwanego sprzętu wojskowego dla Sił Zbrojnych Rzeczypospolitej Polskiej, a w pkt 3 sprawy bieżące.

Otwieram posiedzenie Komisji. Stwierdzam kworum oraz przyjęcie protokołu z 39. posiedzenia, wobec niewniesienia do niego zastrzeżeń.

Witam zaproszonych gości, a przede wszystkim pana ministra Bartosza Kownackiego sekretarza stanu w Ministerstwie Obrony Narodowej pana pułkownika Sławomira Augustyna szefa Inspektoratu Implementacji Innowacyjnych Technologii Obronnych, pana pułkownika Tomasza Żyto pełniącego obowiązki szefa Inspektoratu Systemów Informacyjnych oraz pana pułkownika Pawła Dziubę doradcę podsekretarza stanu w Ministerstwie Obrony Narodowej. Witam wszystkich gości.

Proszę państwa, jeżeli nie ma uwag do porządku obrad – a nie widzę zgłoszeń – poproszę pana ministra o przedstawienie informacji.

Sekretarz stanu w Ministerstwie Obrony Narodowej Bartosz Kownacki:

Panie przewodniczący, Wysoka Komisjo, przepraszam za opóźnienie. To jest kwestia siły wyższej. Tak więc mam nadzieję, że te kilka minut będzie mi wybaczone. Jak pan przewodniczący powiedział, na dzisiejszym posiedzeniu Komisji mamy dwa bardzo ważne tematy. Pierwszy dotyczy systemów teleinformatycznych, a więc jednej z najważniejszych spraw w Ministerstwie Obrony Narodowej. Sprawy, która jest objęta szczególnym priorytetem i została uwzględniona również w zmienionym programie modernizacji technicznej polskiej armii. A co najważniejsze, jest to sprawa, która była szeroko dyskutowana w trakcie ostatniego szczytu NATO. Ze względu na jej wagę dla bezpieczeństwa państwa poproszę, żeby informacja została przekazana przez osobę, która będzie naj-

bardziej kompetentna w tym zakresie, czyli przez szefa Inspektoratu Systemów Informacyjnych pana pułkownika Tomasza Żyto.

Przewodniczący poseł Michał Jach (PiS):

Proszę bardzo.

Czasowo p.o. szefa Inspektoratu Systemów Informacyjnych płk Tomasz Żyto:

Panie przewodniczący, szanowna Komisjo, szanowni państwo, pozwolę sobie państwu odczytać, czy przedstawić podstawowe i jawne informacje dotyczące tego, o czym mówił pan minister Kownacki, czyli generalnie systemu bezpieczeństwa teleinformatycznego sił zbrojnych. Otóż, proszę państwa, ten system jest jednym z wielu systemów wpływających na funkcjonowanie resortu obrony narodowej. Wynika on przede wszystkim z ustawy o ochronie informacji niejawnych oraz z najlepszych praktyk w dziedzinie cyberbezpieczeństwa. Jego architektura została przedstawiona na slajdzie. Składa się ona z pięciu fundamentalnych filarów. Pierwszym jest system planowania i programowania rozwoju sił zbrojnych, w którym my, jako wojsko, ujmujemy w wieloletniej perspektywie rozwój systemów teleinformatycznych oraz rozwój systemów bezpieczeństwa w aspekcie techniki, organizacji, ale również finansów.

Oczywiście, kolejny taki filar, to same systemy teleinformatyczne, które dostarczają informacje i wiedzę na poszczególne szczeble kierowania i dowodzenia oraz narzędzia, które wspierają ciągłość działania oraz wiarygodność i aktualność informacji. Trzeci filar, to oczywiście system reagowania na incydenty komputerowe sił zbrojnych. To jest taki zasadniczy element bezpieczeństwa. Jest to system, który obejmuje organizacyjnie i technicznie rozwiązania monitorowania poziomu bezpieczeństwa oraz reagowania na zdarzenia. Czwarty filar to narodowy potencjał kryptograficzny, który zapewnia nam utrzymanie zdolności w zakresie wymaganego poziomu poufności informacji w systemach teleinformatycznych poprzez zastosowanie różnego rodzaju technik i urządzeń do programowania kryptograficznego.

Oczywiście, jest też piąty, zasadniczy filar w kontekście zobowiązań sojuszniczych. Zobowiązania sojusznicze w ramach NATO obligują kraje Sojuszu do utrzymania i podnoszenia poziomu bezpieczeństwa własnych sieci i systemów teleinformatycznych. Odwołam się tu chociażby do tej piątej domeny operacyjnej, jako do jednego z ważnych dla nas ustaleń szczytu NATO w Warszawie. Drodzy państwo, poza licznymi działaniami istotnymi dla rozwoju i utrzymania systemu bezpieczeństwa teleinformatycznego, jest także doskonalenie różnych aspektów funkcjonowania sił zbrojnych. Podkreślę tu przede wszystkim doskonalenie struktur organizacyjnych dla bezpieczeństwa, odpowiedzialnych za skuteczność i efektywność działania tego systemu bezpieczeństwa. Podkreślę kwestie edukacji dla bezpieczeństwa. Podkreślę kwestie współpracy dla bezpieczeństwa. Podkreślę sprawę standaryzacji, ale również – co jest ważne dla nas, dla praktyków – praktycznej weryfikacji posiadanych zdolności w zakresie bezpieczeństwa teleinformatycznego w formule bieżących działań w sytuacji realnych zagrożeń, które funkcjonują dziś we współczesnym świecie, jak również dedykowanych bezpieczeństwu ćwiczeń lub ich epizodów, które realizujemy w ciągu roku.

Szanowni państwo, oczywiście, wszystkie powyższe elementy nie są jedynymi składowymi systemu bezpieczeństwa teleinformatycznego, niemniej jednak determinują szeroko rozumianą jakość tego podsystemu i jego gwarancje w zakresie ochrony i obrony. W dalszej części pozwolę sobie na krótką charakterystykę poszczególnych filarów i ich aspektów bezpieczeństwa. Proszę państwa, jeżeli chodzi o system planowania i programowania, to jest to system, który pozwala siłom zbrojnym rozwijać się w różnych formach, kształtach i służbach. W ramach obowiązującego systemu programowania i planowania rozwoju sił zbrojnych jako części procesu planowania obronnego wprowadzone zostały zagadnienia związane z cyberbezpieczeństwem. Kierunkowe ustalenia – co tutaj podkreślę – zostały wprowadzone do aktualnego programu rozwoju sił zbrojnych, jak również są uwzględniane w pracach nowej perspektywy planistycznej na lata 2017-2026. Powyższe ustalenia zapewniły szczegółowe rozwinięcie kluczowych domen systemu bezpieczeństwa teleinformatycznego w zasadniczych dokumentach planistycznych. Podkreślę tutaj 2. Rozpoczęto prace, które trwają, nad planem rozwoju obrony cybernetycznej,

cyberbezpieczeństwa oraz zapewnienia bezpieczeństwa kryptologicznego na kolejną perspektywę planistyczną.

Podkreślę również opracowany w tym roku i zatwierdzony program operacyjny osiągnięcia zdolności operacyjnej w zakresie bezpieczeństwa w cyberprzestrzeni i wsparcia kryptologicznego, jako kolejny program operacyjny w siłach zbrojnych. W ujęciu budżetu państwa zagadnienia bezpieczeństwa teleinformatycznego są planowane w funkcji 11 – Budżet zadaniowy, bezpieczeństwo zewnętrzne i nienaruszalność granic, podzadania zdolność do dowodzenia siłami zbrojnymi oraz informatyzacja, kierowanie i zarządzanie resortem obrony narodowej. Oczywiście, szczegółowe zadania ujmowane są w planach specjalistycznych, a w szczególności w centralnych planach rzeczowych, czy w planie modernizacji technicznej.

Systemy teleinformatyczne, jako drugi filar rozwoju systemu bezpieczeństwa teleinformatycznego resortu obrony narodowej. Podkreślę, że w resorcie funkcjonuje kilkanaście zasadniczych, kluczowych rozległych systemów teleinformatycznych, które dostarczają narzędzia wspierające wykonywanie zadań w czasie pokoju, kryzysu i wojny. W codziennej służbie zabezpieczają bieżące funkcjonowanie komórek i jednostek organizacyjnych w różnych aspektach ich działania, od wymiany dokumentów elektronicznych, przez wymianę interpersonalną, zabezpieczenie służb finansowych, logistycznych, czy szkolenia lotniczego, aż po szczególne funkcje, jak obrona powietrzna. Podkreślę, że swoim zasięgiem obejmuje to terytorium kraju, ale również – oczywiście – jednostki zlokalizowane poza jego granicami. Pod względem technologicznym stanowią bardzo heterogeniczne środowisko, w którym zapewniane są użytkownikom zintegrowane usługi teleinformatyczne. Możliwości użytkowanych systemów w zakresie dostarczanych funkcji i informacji, jak również ich stan bezpieczeństwa ma dzisiaj wpływ na jakość procesu dowodzenia i kierowania w resorcie obrony narodowej. Stąd rozwój i utrzymanie tych systemów podlega szczególnej uwadze.

Jak wskazano na wstępie, zasadniczą działalność resortu prowadzimy w segmencie systemów niejawnych, a ich cechą szczególną jest praktyczna fizyczna separacja od struktur otwartych, publicznie dostępnych, przy czym – oczywiście – podstawą bezpieczeństwa tych systemów nie jest tylko ich fizyczna izolacja. W tym względzie wskazać należy na kluczowe rozwiązania. Jak zaznaczono, cechą szczególną systemu jest bazowanie na wydzielonych łączach telekomunikacyjnych własnych oraz dzierżawionych od operatorów telekomunikacyjnych i kreowanie w zasobach wymaganych relacji. Jest to możliwe dzięki posiadaniu własnych węzłów łączności oraz dużych kompetencji w resorcie w zakresie telekomunikacji.

Odnotować należy, że bieżące działania w zakresie utrzymania systemu telekomunikacyjnego skupiają się na optymalizacji wykorzystywanych łączy, wprowadzaniu nowych standardów technologicznych, procedurach do ubiegania i usuwania awarii, monitoringu posiadanego zasobu teletransmisyjnego, uzyskaniu wysokiego poziomu niezawodności, gwarancjach umownych, w tym rozbudowy infrastruktury telekomunikacyjnej o nowe, niezależne dowiązania obiektów resortu. Drugą cechą tych systemów teleinformatycznych jest finalizowany na koniec bieżącego roku projekt wdrożenia jednolitej warstwy transportowej IP w technologii MPLS. Projekt dla sił zbrojnych zapewnia optymalizację przydzielania zasobów w zależności od dynamicznie zmieniających się potrzeb oraz zwiększa odporność na awarię.

Trzeci, równie istotny projekt z punktu widzenia zachowania bezpieczeństwa danych, realizowany również na koniec tego roku, to projekt uruchomienia resortowego centrum archiwizacji danych, który wpisuje się w realizowaną od kilku lat w resorcie koncepcję resortowej chmury obliczeniowej. Czwarty obszar szczególnej uwagi, to – oczywiście – systemy informatyczne i oprogramowanie produkowane własnymi siłami resortu. Pozyskujemy także i wdrażamy w systemach odpowiednie rozwiązania z rynku cywilnego. Wymagamy dzisiaj od tego oprogramowania nie tylko określonych funkcji, ale również atrybutów bezpieczeństwa, a więc m.in. zapewnienia skutecznej kontroli dostępu, czy szczegółowej rozliczalności z uzyskiwanego dostępu.

Piątym kierunkiem naszych działań jest praktyczna ocena ryzyka dla systemów teleinformatycznych, wynikająca z informacji uzyskiwanych z wdrażanych systemów moni-

torowania, korelacji i badań. I w końcu szósty, istotny w kontekście zachowania ciągłości działania systemów teleinformatycznych zorganizowanych i doskonalonych w resorcie, system wsparcia technicznego zapewniający kompleksową obsługę zdarzeń zgłoszonych przez użytkowników systemów, jak również przez użytkowane w resorcie systemy. Podkreślę, że nie bez znaczenia w części systemów teleinformatycznych dla jakości procesu eksploatacji tych systemów oraz bezpieczeństwa przetwarzanych danych jest zorganizowana trójpoziomowa struktura administratorów, która ma wymiar lokalny, regionalny i centralny. Centralną rolę pełni Inspektorat Systemów Informacyjnych, jako organizator zasadniczych rozległych systemów teleinformatycznych w resorcie oraz prowadzący bardzo dobrą współpracę w tym zakresie ze Służbą Kontrwywiadu Wojskowego oraz z Narodowym Centrum Kryptologii.

Dodatkowej informacji wymaga użytkowany w resorcie zasadniczy system jawny, dotychczas INTERMON, rozwijany i doskonalony jako platforma MILNET-I (od Internet). Od roku ten system podlega intensywnej przebudowie, zarówno w warstwie dostępu do internetu, jak i organizacji świadczonych usług oraz porządkowaniu architektury programowej. System ten ze swej natury wymaga podłączenia do internetu, co podkreślę, przez co podlega znanym zagrożeniom, przez co jest również wykorzystywany wizerunkowo. System reagowania na incydenty komputerowe, to trzeci filar systemu bezpieczeństwa. Ten system to zasadniczy filar systemu bezpieczeństwa, powołany formalnie w resorcie obrony narodowej w 2008 r. Jest zorganizowany w strukturze trzypoziomowej, w skład której wchodzi centrum koordynacyjne, którego funkcje spełnia właściwa komórka Służby Kontrwywiadu Wojskowego, centrum wsparcia, którego funkcje wypełnia wewnętrzna komórka Narodowego Centrum Kryptologii oraz administratorzy systemów informatycznych, w tym Inspektorat Systemów Informacyjnych oraz administratorzy systemów w jednostkach i komórkach organizacyjnych.

System obsługuje zarówno systemy przetwarzające informacje jawne oraz niejawne. Podstawowym elementem systemu reagowania na incydenty komputerowe odpowiedzialnym za bezpośrednie reagowanie na incydenty są administratorzy systemów teleinformatycznych, głównie ze struktur podległych właśnie Inspektoratowi Systemów Informacyjnych. Dzięki dobrze zorganizowanej współpracy ww. elementów składowych systemu, możliwe jest skuteczne realizowanie procesu obsługi incydentów komputerowych w siłach zbrojnych. Nadzór nad funkcjonowaniem tego systemu w odniesieniu do systemów teleinformatycznych przeznaczonych do przetwarzania informacji niejawnych sprawuje pełnomocnik ministra obrony narodowej do sprawa bezpieczeństwa cyberprzestrzeni, a w odniesieniu do systemów niejawnych Służba Kontrwywiadu Wojskowego.

Podkreślę, że ten system, który jest przedstawiany, jest zorganizowany na wzór analogicznego zespołu działającego w strukturach NATO – Computer Incident Response Capability Team. Poza specjalistami z dziedziny bezpieczeństwa oraz administratorami systemów informatycznych wchodzącymi w skład struktur bezpieczeństwa Ministerstwa Obrony Narodowej, kluczową rolę w zapewnieniu właściwego poziomu bezpieczeństwa odgrywają wykorzystywane technologie bezpieczeństwa teleinformatycznego widoczne na rysunku, jak chociażby systemy: ochrony antywirusowej, wykrywania i blokowania włamań, aktualizacji oprogramowania, zapór sieciowych, szyfrowania, ochrony przed wyciekiem danych, analizy kodu złośliwego, skanowania i wykrywania podatności, koordynacji zdarzeń, informatyki śledczej, a także wiele innych.

Kolejnym, czwartym filarem jest coś, co można określić, jako narodowy potencjał kryptograficzny. Sprawne zarządzanie kryptografią jest dzisiaj kluczowym filarem zapewnienia bezpieczeństwa teleinformatycznego w siłach zbrojnych. Obowiązujące ramy prawne stosowania rozwiązań kryptograficznych zapewniają ochronę narodowych informacji niejawnych oraz informacji sojuszniczych. Organami wykonawczymi zabezpieczenia kryptograficznego są komórki bezpieczeństwa systemów łączności i informatyki, funkcjonujące w jednostkach organizacyjnych resortu różnych szczebli. Zapewniają one sprawne funkcjonowanie systemów ochrony kryptograficznej. Narodowe Centrum Kryptograficzne, zgodnie ze swoim statutem, konsoliduje kompetencje i zasoby resortu w obszarze kryptologii, a w szczególności określa kierunki rozwoju systemów kryptogra-

ficznych, a jako gestor urządzeń i narzędzi kryptologicznych koordynuje zabezpieczenie potrzeb sił zbrojnych w tym zakresie.

Podkreślę, że w odniesieniu do tego narodowego potencjału kryptograficznego dostarczanie nowoczesnych krajowych rozwiązań kryptograficznych stało się dziś kluczowe dla obronności i bezpieczeństwa państwa. Z powodzeniem prowadzone są w tym względzie prace wdrożeniowe i eksploatacyjne. Odnotuję tutaj współpracę z krajowymi ośrodkami naukowo-badawczymi i z krajowym przemysłem, czego materialnym wyrazem są projekty prowadzone w ramach Narodowego Centrum Badań i Rozwoju. Ścisła współpraca ze strukturami Sojuszu pozwoli, również w niedalekiej przyszłości, wdrożyć do sił zbrojnych standardy kryptograficzne rozwijane w NATO w ramach transformacji kryptograficznej, umożliwiając tym samym zapewnienie interoperacyjności kryptograficznej przy wykorzystaniu krajowych rozwiązań sprzętowych. W ramach współpracy międzynarodowej realizowane są w tym obszarze działania mające na celu przystąpienie Polski do partnerstwa łączności i informatyki pomiędzy ministrem obrony narodowej, a Agencją Łączności i Informatyki NATO, NCIA. Spodziewamy się, że w tym roku zostanie podpisane stosowne porozumienie w tym zakresie.

Struktury organizacyjne dla bezpieczeństwa, jako bardzo ważny aspekt budowania poszczególnych filarów. W resorcie obrony narodowej funkcjonują sprawne struktury organizacyjne odpowiedzialne za bezpieczeństwo teleinformatyczne. Zasadniczymi ogniwami tej struktury są – oczywiście – Służba Kontrwywiadu Wojskowego, Narodowe Centrum Kryptologii, Inspektorat Systemów Informacyjnych, jako organizator zasadniczych, kluczowych, rozległych systemów teleinformatycznych w resorcie obrony narodowej oraz Departament Ochrony Informacji Niejawnych, wypełniający ustawowe zadania pionu ochrony informacji niejawnych Ministerstwa Obrony Narodowej. Dopełnieniem powyższych są struktury występujące praktycznie w każdej jednostce organizacyjnej. Są to piony ochrony informacji niejawnych, administratorzy lokalni użytkowanych w jednostce systemów, w większości rozległych i resortowych oraz występujące w części jednostek organy bezpieczeństwa łączności i informatyki dedykowane tylko i wyłącznie systemom kryptograficznym.

Podkreślić należy, że w resorcie powołany jest pełnomocnik Ministra Obrony Narodowej do spraw bezpieczeństwa cyberprzestrzeni. Zadania w tym względzie powierzono podsekretarzowi stanu w Ministerstwie Obrony Narodowej panu Bartłomiejowi Grabskiemu. Kolejny slajd, to kolejny ważny aspekt edukacja dla bezpieczeństwa. Budowa kapitału ludzkiego w dziedzinie cyberbezpieczeństwa jest – oczywiście – wartością samą w sobie. W tym względzie resort podejmuje wielokierunkowe działania, których celem jest z jednej strony posiadanie wysoko wykwalifikowanego personelu w dziedzinie informatyki, kryptologii i cyberbezpieczeństwa, a z drugiej strony posiadanie świadomych istniejących zagrożeń użytkowników systemów. Podkreślić należy, że w istniejącym systemie kształcenia w wojskowym szkolnictwie wyższym, zabezpieczającym potrzeby w zakresie pozyskania kadr o specjalnościach informatyka, kryptologia i cyberbezpieczeństwo zwiększono stosowne limity przyjęć na kolejne lata. Z kolei personel pozostający już w służbie kierowany jest na wysoko specjalizowane szkolenia zarówno w ośrodkach krajowych, jak i zagranicznych.

Oczywiście, prowadzony jest proces edukacji dla kadry i pracowników wojska w zakresie bezpieczeństwa teleinformatycznego. W ramach tej działalności, w ramach której prowadzone są szkolenia, prowadzimy wewnętrzne portale poświęcone kwestiom bezpieczeństwa, jak również publikowane są jawne i niejawne biuletyny. Nie bez znaczenia dla bezpieczeństwa są również ustawiczne szkolenia użytkowników, jako najsłabszego ogniwa bezpieczeństwa, do obsługi wdrażanych i eksploatowanych systemów teleinformatycznych. W proces szkolenia angażowana jest stopniowo i wdrażana – a w zasadzie już wdrożona w siłach zbrojnych – platforma nauczania na odległość. Nasze doświadczenia wskazują, że działania edukacyjne w połączeniu z wysokimi zdolnościami w zakresie technicznej analizy incydentów komputerowych są kluczowe dla utrzymania właściwego poziomu bezpieczeństwa teleinformatycznego sił zbrojnych.

Kolejny aspekt, to współpraca dla bezpieczeństwa. Tutaj krótko odnotuję, że na rzecz bezpieczeństwa teleinformatycznego sił zbrojnych realizowana jest współpraca krajowa

i międzynarodowa z podmiotami publicznymi oraz z sektora prywatnego. W tym względzie podkreślę współpracę z przedsiębiorstwami telekomunikacyjnymi oraz podmiotami sektora prywatnego, uczestniczącymi w realizacji na rzecz sił zbrojnych infrastrukturalnych projektów w dziedzinie IT – w szczególności chodzi tu o zasoby telekomunikacyjne – współdziałanie z największymi zespołami reagowania na incydenty komputerowe w Polsce oraz z zespołami CIRT NATO. Oczywiście, uczestnictwo w pracach międzynarodowych grup roboczych w zakresie cyberbezpieczeństwa, rozwoju systemów i technologii informatycznych oraz udział takich prac w praktycznych krajowych i międzynarodowych ćwiczeniach z zakresu bezpieczeństwa teleinformatycznego oraz interoperacyjności systemów informatycznych, o czym powiem później.

Kolejny aspekt, to standaryzacja dla bezpieczeństwa. Aspekt standaryzacji formalnej i de iure odgrywa istotną rolę w rozwoju i utrzymaniu systemów teleinformatycznych i bezpieczeństwa teleinformatycznego. Oczywiście, proces standaryzacji trwa. Podlegają mu pozyskiwane technologie teleinformatyczne, począwszy od sprzętu teleinformatycznego, oprogramowania, poprzez stosowane wystandaryzowane profile konfiguracji użytkowanego sprzętu i oprogramowania w systemach, aż po zunifikowane procedury użytkowania i bezpieczeństwa. W tym ostatnim względzie w ostatnim czasie zakończono prace nad aktualizacją podręczników systemu reagowania na incydenty komputerowe oraz standardowych procedur operacyjnych w tym zakresie. Ze swojej strony mogę powiedzieć, że w standaryzacji tych technologii i procedur dostrzegamy duży potencjał eliminujący znaczną część zagrożeń, jak również istotnie skracający czas reakcji na zachodzące zdarzenia.

Kolejny, już przedostatni aspekt, a w zasadzie już ostatni. Przykłady dla bezpieczeństwa, czy praktyczna weryfikacja bezpieczeństwa. Oczywiście, system, który jest dzisiaj, funkcjonuje. Rozwijamy go. Podlega ustawicznej weryfikacji w ramach codziennej, bieżącej ochrony zasobów resortu – bo to trwa – które podlegają zagrożeniom. Oczywiście planowana jest formuła ćwiczeń, treningów i warsztatów. Na podkreślenie zasługuje aktywne i wielokrotnie bardzo dobrze oceniane uczestnictwo sił zbrojnych w największym na świecie technicznym ćwiczeniu w zakresie cyberobrony Locked Shields, organizowanym przez centrum doskonalenia cybernetycznego w Tallinie. Prawie bez ustanku plasujemy się w tym ćwiczeniu „na pudle". Jest też ćwiczenie interoperacyjności The Coalition Warrior Interoperability Exercise CIWIX organizowane przez sojusznicze dowództwo transformacji, zresztą na arenie naszego kraju.

W najbliższych miesiącach planowany jest udział specjalistów do spraw cyberbezpieczeństwa w dwóch kolejnych ćwiczeniach. Cyber Coalition 16, to ćwiczenia organizowane przez sojusznicze dowództwo do spraw transformacji. Ćwiczenie Crossed Swords 17 będzie organizowane przez centrum doskonalenia cybernetycznego w Tallinie. Przewidziany jest również udział w wielu treningach organizowanych w resorcie obrony narodowej, w trakcie których symulowane są zagrożenia występujące w cyberprzestrzeni. Na zakończenie tego aspektu współdziałania wielu podmiotów z zakresu bezpieczeństwa teleinformatycznego sił zbrojnych oraz jednostek państw sojuszniczych, dobrym przykładem było zakończone sukcesem w tym zakresie ćwiczenie Anakonda 16, w trakcie którego przeprowadzano epizody realnych zagrożeń w cyberprzestrzeni.

Na zakończenie tego aspektu odnotuję również bardzo dobrą organizację systemu łączności i informatyki oraz zapewnienie jego bezpieczeństwa na potrzeby organizacji szczytu NATO w Warszawie i współpracę w tym zakresie Agencji Bezpieczeństwa Wewnętrznego z jednostkami Ministerstwa Obrony Narodowej takimi, jak: SKW, NCK oraz Inspektorat Systemów Informacyjnych. Szanowni państwo, podsumowując moje krótkie wystąpienie powiem, że kierownictwo resortu obrony narodowej dostrzega wagę i wpływ cyberprzestrzeni na realizację zadań przez siły zbrojne. Dokonujące się we współczesnym świecie zmiany technologiczne, których beneficjantem są również siły zbrojne, powodują z jednej strony skok jakościowy procesów kierowania i dowodzenia, a z drugiej strony przynoszą jednak nowe zagrożenia nie tylko dla sił zbrojnych. Stąd potrzeba i konieczność rozwijania potencjału wojska w dziedzinie cyberbezpieczeństwa.

Temu służyły decyzje podjęte w ostatnim roku przez kierownictwo resortu. Dotyczyły one m.in. wzmocnienia Narodowego Centrum Kryptologii, ścisłej współpracy Biura

Bezpieczeństwa Cybernetycznego Służby Kontrwywiadu Wojskowego, Narodowego Centrum Kryptologicznego i Inspektoratu Systemów Informacyjnych, pracy z wieloletnimi planami w dziedzinie informatyzacji, kryptologii i cyberbezpieczeństwa, pracy z programem operacyjnym w dziedzinie kryptologii i bezpieczeństwa oraz wielu innych działań, których celem jest osiąganie kolejnych i doskonalenie zdobytych zdolności w tej złożonej dziedzinie. W tym względzie szczególnie istotne są te główne kierunki, które chcemy osiągnąć: budowa przez siły zbrojne zdolności do obrony i ochrony własnych systemów teleinformacyjnych i zgromadzonych w nich zasobów, budowa zdolności do aktywnej obrony i działań ofensywnych w cyberprzestrzeni, tworzenie i wzmacnianie struktur przeznaczonych do realizacji zadań w cyberprzestrzeni dysponujących zdolnościami w zakresie rozpoznania, zapobiegania i zwalczania cyberzagrożeń, rozbudowa potencjału systemu reagowania na incydenty komputerowe, w szczególności poprzez rozwój kompetencji dziedzinowych i współpracę z partnerskimi zespołami reagowania na incydenty komputerowe.

Będzie to także konsekwentna realizacja postanowień szczytu NATO w Warszawie w zakresie cyberbezpieczeństwa, a więc piąta domena działań operacyjnych i – oczywiście – zapewnienie stałego podnoszenia świadomości personelu resortu w zakresie współczesnych cyberzagrożeń. Na zakończenie mojego wystąpienia chcę podkreślić, że nie bez znaczenia dla rozwoju zdolności w zakresie informatyki, kryptologii i cyberbezpieczeństwa będzie również stworzenie warunków konkurencyjności w stosunku do rynku cywilnego dla tych poszukiwanych specjalności zawodowych, poszukiwanych również na rynku cywilnym. Dziękuję bardzo, panie przewodniczący i panie ministrze.

Przewodniczący poseł Michał Jach (PiS):

Dziękuję bardzo, panie pułkowniku. Otwieram dyskusję. Proszę o zgłaszanie się. Pani poseł Anna Siarkowska.

Poseł Anna Maria Siarkowska (Kukiz15):

Bardzo dziękuję, panie przewodniczący. Panie ministrze, Wysoka Komisjo, wysłuchaliśmy wystąpienia, które – mam wrażenie – jest raczej formą wykładu. Informacje, które otrzymaliśmy, są raczej informacjami, które z powodzeniem można było wyszukać w internecie. Można powiedzieć, że był to poziom pierwszych lat studiów. Zdecydowanie zabrakło konkretów. Po tym wystąpieniu tak naprawdę wiem tyle samo, ile wiedziałam przychodząc do tej sali na posiedzenie Komisji. A więc jest w ogóle pytanie o sens tego wystąpienia. O to, że posłowie poświęcają swój czas, żeby tych informacji wysłuchać.

A teraz, jeżeli chodzi o konkrety. Jeżeli nawet posłowie wysłuchują informacji i oczekują podania faktów na temat działań podjętych przez Ministerstwo Obrony Narodowej w zakresie ochrony, czy w ogóle wzmocnienia bezpieczeństwa teleinformatycznego, a jedyne, co słyszą, to np. tego typu elementy, że nastąpiło wzmocnienie centrum kryptologicznego, albo że nastąpiły jakieś prace w dziedzinach kryptologii i cyberbezpieczeństwa, ale w ogóle nie wiadomo, jakie to prace i na czym polegały, to naprawdę uważam, że ta informacja nie tyle była uboga, co praktycznie żadna.

Druga kwestia. Tu w takim razie zapytam o pewien konkret, który akurat mnie bardzo interesuje. Może chociaż w tym aspekcie są państwo w stanie udzielić nam informacji. Wiem, że w dniach 24-25 września br. na terenie Cytadeli Warszawskiej odbyło się ćwiczenie organizowane przez biuro do spraw utworzenia obrony terytorialnej. Było to ćwiczenie, w ramach którego pracownicy biura razem z członkami organizacji proobronnych prowadzili działania. To było szkolenie, które dotyczyło cyberobrony terytorialnej. Tak to można nazwać. I teraz jest pytanie. Czy mogliby państwo nam przybliżyć, na czym polegało to szkolenie i jakie są wnioski z tego szkolenia? Chociażby tylko w takim jednym małym aspekcie. A co do reszty, już się wypowiedziałam na początku. Uważam, że posłowie z tego posiedzenia Komisji wyjdą z takim samym poziomem informacji, z jakim na nie weszli. Bardzo dziękuję.

Przewodniczący poseł Michał Jach (PiS):

Dziękuję, pani poseł. Proszę, pan poseł Piotr Pyzik.

Poseł Piotr Pyzik (PiS):

Dziękuję bardzo. Podzielając zdanie mojej poprzedniczki, pani poseł, skupię się na konkretnym temacie. Chciałem zapytać o odsetek cywilnych pracowników wśród administratorów systemów teleinformatycznych. Czy dążeniem sił zbrojnych jest zwiększenie nawet do 100% zawodowych wojskowych na stanowiska administratorów? W praktyce miałem możliwość przekonać się o tym osobiście, że to szeregowi administratorzy systemów teleinformacyjnych są pierwszą linią obrony na cyberfroncie. Doświadczenia w dziedzinie cyberbezpieczeństwa wskazują, że najczęściej zawodzi czynnik ludzki. Wydaje się, że związane z mundurem poczucie służby i misji będzie najlepszym gwarantem zaangażowania administratorów oraz dochowania tajemnicy służbowej. Oczywiście, w połączeniu z regularnymi szkoleniami, a także kontaktami branżowymi z administratorami z sektorów cywilnych. Dziękuję uprzejmie.

Przewodniczący poseł Michał Jach (PiS):

Dziękuję. Więcej zgłoszeń nie widziałem. Bardzo proszę, panie ministrze, o odpowiedź na pytania.

Sekretarz stanu w MON Bartosz Kownacki:

Panie przewodniczący, zanim oddam głos powiem, że pytania pana posła Pyzika było bardzo konkretne. Nie wiem, czy będą dokładne dane, żeby odpowiedzieć. Akurat, pani poseł, ja nie podzielam tego zdania. Nikt nie chciał zmarnować tak cennego czasu parlamentarzystów. Ale musimy też mieć świadomość, że wiele informacji, które padają na posiedzeniach Komisji Obrony Narodowej, musi mieć charakter ogólny, bo musielibyśmy rozmawiać w innych warunkach, żeby rozmawiać o szczegółach.

Poseł Anna Maria Siarkowska (Kukiz15):

To rozmawiajmy.

Sekretarz stanu w MON Bartosz Kownacki:

Wtedy będzie można powiedzieć dużo więcej. Pani poseł, nie wszystko można tak przedstawić, jak czasem byśmy tego chcieli. Jeżeli będzie potrzeba, to można później dostać tę informację na piśmie, odpowiednio opieczętowaną i oklauzulowaną. Po to są konkretne pytania. Tutaj był pewien zaczątek do dyskusji, którą możemy przeprowadzić. Jeżeli sprawa jest rzeczywiście szczególnej wagi, to możemy dyskutować w odpowiednim innym pomieszczeniu, które pozwala na taką rozmowę. Proszę też to zawsze brać pod uwagę. Jeżeli chodzi o szczegóły, to oddam głos panu pułkownikowi.

Szef inspektoratu płk Tomasz Żyto:

Jak powiedział pan minister, ta dzisiejsza informacja jest pewnym wyważeniem pomiędzy tym, co jest jawne, a tym, co jest niejawne. Myślę, że ta informacja jednak zawiera pewne fakty. Mówiliśmy tutaj o tym, że jest wzmocnienie. Mówiliśmy o tym, że jest program operacyjny itd., itd., więc to są pewne fakty. Natomiast nie jestem w stanie przedstawić państwu w formule jawnej prezentacji danych, które fizycznie są po prostu niejawne. To jest pierwsza sprawa. Natomiast, wychodząc naprzeciw temu pytaniu, jeżeli chodzi o te ćwiczenia, o które pani pytała, to jest właśnie to, co mówiliśmy o tym aspekcie, o edukacji dla bezpieczeństwa. Takie ćwiczenia, czy szkolenia odbywają się. To nie jest jakiś akt jednorazowy, ale pewien proces. W szczegółach nie jest dzisiaj istotne, czy to było ćwiczenie tylko dla pracowników. A te wnioski są jednoznaczne. Podnosimy ten poziom edukacji od niepamiętnych lat i ten proces będzie trwał. Powiedziano dzisiaj, że ten użytkownik jest najsłabszym ogniwem w tym systemie. Dlatego ten proces edukacji będzie trwał cały czas. To tyle, jeżeli chodzi o kwestie szkolenia, czy jakiegokolwiek ćwiczenia w zakresie biura do spraw tworzenia wojsk obrony terytorialnej na terenie Cytadeli.

Natomiast, jeżeli chodzi o pracowników wojska, to myślę, że podniesiony został bardzo ważny aspekt, o którym także mówiliśmy – czy jesteśmy konkurencyjni w stosunku do sektora cywilnego. Było pytanie, ilu mamy dzisiaj informatyków – pracowników wojska. Gdybyśmy wzięli ponadzakładowy układ zbiorowy pracy, to liczba stanowisk informatyków, czy osób oznaczonych o takiej specjalności, to – drodzy państwo – ok. 500. Czy to są wszyscy informatycy pracownicy wojska? Na pewno nie, bo są jeszcze samoza-

trudnienia. Ale jest to mniej więcej skala pracowników wojska – co zaznaczam – którzy są przypisani do specjalności – informatyk. Natomiast, nie są to – oczywiście – jedyni administratorzy. To nie jest jedyny personel, który zajmuje się informatyką, czy bezpieczeństwem w Wojsku Polskim. Tych ludzi jest zdecydowanie więcej. Zaznaczę, że w każdej jednostce wojskowej są chociażby piony ochrony. Są inspektorzy, są administratorzy. No i cała struktura Inspektoratu Systemów Informacyjnych. Drodzy państwo, jest to struktura, która ma 5 tys. ludzi. Ta taka jest mniej więcej skala zjawiska, czy organizacji, która w całości zajmuje się kwestią rozwoju i utrzymania szeroko rozumianych systemów teleinformatycznych w strukturze stacjonarnej w kraju i za granicą. Dziękuję, panie przewodniczący.

Przewodniczący poseł Michał Jach (PiS):

Dziękuję. Pan poseł Bejda. Proszę bardzo.

Poseł Paweł Bejda (PSL):

Panie przewodniczący, mam takie pytanie. Odpowiedź na to pytanie będzie skutkowała moim następnym pytaniem, które chcę zadać. Moje pytanie brzmi tak. Kto był inicjatorem wprowadzenia tej informacji na dzisiejsze posiedzenie Komisji? Czy to był pan przewodniczący, czy strona rządowa?

Przewodniczący poseł Michał Jach (PiS):

To było przyjęte przez Komisję zgodnie z planem na wniosek Ministerstwa Obrony Narodowej.

Poseł Paweł Bejda (PSL):

W takim razie następna część mojego pytania, a właściwie prośby. Jest to prośba do strony rządowej, do pana ministra. Jeżeli naprawdę państwo nie możecie nam przedstawić pewnych konkretów, to albo utajnijcie to spotkanie, albo po prostu powiedzcie, że nie chcecie wypowiadać się na ten temat. Traktujmy się poważnie. Nie traktujcie nas, posłów, jako kogoś, kto wam ewentualnie przeszkadza. Traktujcie nas poważnie, a nie jak dzieci w piaskownicy. Taka jest moja prośba.

Przewodniczący poseł Michał Jach (PiS):

Pan minister Cezary Grabarczyk. Proszę.

Poseł Cezary Grabarczyk (PO):

Dziękuję bardzo. Panie przewodniczący, panie ministrze, panowie oficerowie, chcielibyśmy jednak uzyskać trochę konkretów, chociaż być może nie na poziomie objętym klauzulami. Jaka jest skala tych szkoleń, o których pan pułkownik informował Komisję? Ilu żołnierzy przeszło te szkolenia? Na jakich kursach? Czy te szkolenia odpowiadają potrzebom? Jak pan pułkownik ocenia realizację w stosunku do potrzeb? Na jaką kwotę opiewają potrzeby dotyczące tej części szkoleń w przyszłym roku? Czy te, które zostały wpisane do projektu budżetu są wystarczające? To jest ten moment, w którym Komisja wsłuchując się w pana referat może udzielić wsparcia. Pracujemy w tej chwili nad budżetem. Łączność, to system nerwowy armii. Sprawna łączność decyduje o skuteczności działań operacyjnych na polu walki. To jest ten moment, w którym panowie możecie upomnieć się o niezbędne środki. Proszę to wykorzystać. Dziękuję.

Przewodniczący poseł Michał Jach (PiS):

Jeszcze raz pani poseł Anna Siarkowska. Proszę.

Poseł Anna Maria Siarkowska (Kukiz15):

Bardzo dziękuję, panie przewodniczący. Panie ministrze, Wysoka Komisjo, mam jeszcze krótkie pytanie uszczegółowiające. Uzyskałam informację odnośnie do ćwiczenia, o które pytałam, że odbyło się w ramach edukacji dla bezpieczeństwa. Jest to dla mnie dość dziwna odpowiedź, żeby nie powiedzieć, że kuriozalna. Wydawało mi się, że zadaniem biura do spraw utworzenia obrony terytorialnej są sprawy koncepcyjne i organizacyjne dotyczące obrony terytorialnej. A zatem wydawałoby się, że takie ćwiczenie powinno raczej mieć charakter pilotażowy, dotyczący właśnie organizacji, czy zadań przyszłej

obrony terytorialnej. I takie było moje przekonanie, że to ćwiczenie było właśnie w takim charakterze organizowane.

Jeżeli odbywałoby się to w ramach edukacji dla bezpieczeństwa, czyli po prostu takiego -jak można powiedzieć – szkolenia różnych grup po prostu tylko dlatego, żeby były bardziej świadome, to jest to wątpliwe, żeby było to tak naprawdę zadanie dla biura do spraw utworzenia obrony terytorialnej. Tego typu zadania powinny wypełniać chociażby takie placówki, jak Akademia Sztuki Wojennej, czy inne uczelnie. Być może powinny to być zadania zlecone. Naprawdę, ta odpowiedź była dla mnie po prostu kuriozalna. Dlatego proszę o wyjaśnienie. Jeżeli jednak miało to taki charakter, o jakim wcześniej mówiłam, czyli takiego pilotażu związanego z przygotowywaniem zadań dla przyszłej obrony terytorialnej, czy kwestii organizacyjnych, to w takim razie prosiłabym też o podanie wniosków z tego ćwiczenia, bo takie wnioski na pewno były sformułowane. Bardzo dziękuję.

Przewodniczący poseł Michał Jach (PiS):

Dziękuję bardzo. Proszę bardzo, panie ministrze i panie pułkowniku.

Sekretarz stanu w MON Bartosz Kownacki:

Panie przewodniczący, szanowna Komisjo, zanim oddam głos panu pułkownikowi, odniosę się jednak do tego, co powiedział pan poseł Bejda. Dlatego, że ta informacja została przedstawiona w taki sposób, w jaki może być z klauzulą „jawne". Nie wszyscy są tak znakomitymi fachowcami, jak pan, panie pośle.

Bardzo dziękuję za pytania pana posła Grabarczyka. Jesteśmy otwarci na te pytania, na które będziemy mogli udzielić odpowiedzi w trakcie dyskusji po prezentacji. I czekamy na takie pytania od pana posła. Jesteśmy dzisiaj gotowi. To nie jest nic nadzwyczajnego, że na te pytania, na które nie można udzielić odpowiedzi na posiedzeniu Komisji, odpowiedzi są udzielane na piśmie. Jestem przekonany, że jest pan świetnie przygotowany. Poza tyradą dotyczącą tego, co chciałby pan usłyszeć, a czego pan nie usłyszał, ma pan wiele pytań, na które na pewno udzielimy panu odpowiedzi. Nie wzdragamy się od tego. W takiej, czy w innej formule na pewno je pan dostanie. Dziękuję bardzo.

Poseł Paweł Bejda (PSL):

Mam do pana taką prośbę, panie ministrze.

Przewodniczący poseł Michał Jach (PiS):

Panie pośle, momencik. Może najpierw pan pułkownik odpowie. Dobrze?

Poseł Paweł Bejda (PSL):

Ale to tylko króciutko, panie przewodniczący.

Przewodniczący poseł Michał Jach (PiS):

No, to proszę bardzo.

Poseł Paweł Bejda (PSL):

Mam tylko taką prośbę, panie ministrze, żeby złośliwości zostawił pan za drzwiami. Dobrze? Niech pan tu przychodzi bez złośliwości i merytorycznie odpowiada na pytania. I tyle.

Sekretarz stanu w MON Bartosz Kownacki:

Panie pośle, o ile pan złoży merytoryczne pytanie, to zostanie udzielona odpowiedź. Pan bierze pieniądze od podatników i przychodząc na posiedzenie Komisji powinien pan wiedzieć, czego pan oczekuje i czego pan się chce dowiedzieć, a nie wygłaszać niemerytoryczne tyrady. Również jestem parlamentarzystą i z przykrością patrzę na tego rodzaju…

Poseł Paweł Bejda (PSL):

Panie ministrze, reprezentuje pan stronę rządową i nie jest pan od pouczania posłów. I niech pan po prostu odstawi te uwagi na bok i tyle. Bo jest pan niegrzeczny.

Przewodniczący poseł Michał Jach (PiS):

Panie pośle, panie pośle. Proszę bardzo, pan pułkownik. Czy tak?

Szef inspektoratu płk Tomasz Żyto:

Tak, jeśli mogę. Panie przewodniczący, szanowni państwo, droga pani poseł, jeżeli chodzi o pani pytanie, proces szkolenia w wojsku nie jest jakimś aktem jednorazowym. Jest to pewien proces, w którym uczestniczą praktycznie wszystkie jednostki. Nie mówię, że dzisiaj, że w każdym dniu odbywa się proces szkolenia, ale jednak ten proces się odbywa. Jest mi tutaj ciężko odnieść się do pani pytania o jednostkowe wydarzenie w biurze do spraw tworzenia obrony terytorialnej. Sądzę, po tym, co pani powiedziała, czy co pani przeczytała w internecie, że ta moja odpowiedź była pełna. To znaczy, jeśli pani przeczytała, że odbyło się jakieś ćwiczenie, czy szkolenie dotyczące cyberobrony, to twierdzę, że to było zaprogramowane w ramach programowego szkolenia uzupełniającego jakieś zagadnienia szkoleniowe, które po prostu tam się odbyły. To jest to wszystko, co mówiłem o edukacji dla bezpieczeństwa. Tam się mieści ten cały proces, który dzisiaj pani ujęła w swoim pytaniu. To tyle, jeśli chodzi o tę kwestię.

Jeżeli chodzi o pytanie pana posła Grabarczyka o proces szkolenia i o to, czy mamy wystarczające pieniądze, czy środki odpowiem, że proces szkolenia jest bardzo wielowymiarowy. Szkolimy się sami z siebie, czyli żołnierz szkoli żołnierza. W każdej jednostce organizacyjnej są piony ochrony. A więc mamy ustawowe obowiązki przeprowadzania wewnętrznych szkoleń. I – oczywiście – są to szkolenia darmowe. Są także szkolenia zewnętrzne, kiedy kupujemy pewnego rodzaju usługi na zewnątrz. Gdybym miał odpowiedzieć na pytanie, ile wojsko, czy ile my, jako informatyka i łączność, wydajemy na te zewnętrzne ćwiczenia komercyjne, to nie pomyliłbym się dużo, gdybym powiedział, że jest to kwota ok. 10 mln zł rocznie. Taki jest mniej więcej koszt komercyjnych szkoleń, wysoko specjalizowanych szkoleń dla specjalistów.

Poseł Cezary Grabarczyk (PO):

I na to wystarcza?

Szef inspektoratu płk Tomasz Żyto:

Tak. To jest mniej więcej taka kwota. Tych szkoleń jest bardzo dużo. Nie jestem w stanie podać państwu w tej chwili dokładnej liczby, ale to jest liczone w tysiącach osób. Ale chcę podkreślić jedną ważną rzecz. Wewnętrznie mamy też zorganizowane grupy wdrożeniowe, czy szkoleniowe, które – jeżeli chodzi o technologie, czy o systemy informatyczne – prowadzą bardzo intensywny proces szkolenia. Praktycznie przez 200 dni w roku – bo tyle mamy praktycznie dni pracy – odbywa się ten proces;. Drodzy państwo, w roku potrafimy przeszkolić 15-18 tys. użytkowników własnymi siłami. Taka jest mniej więcej skala tego zjawiska. Gdybyśmy mieli kupować takie usługi na zewnątrz, to – oczywiście – koszty byłyby zdecydowanie większe. Mówię tutaj o szkoleniach wysoko specjalizowanych w technologiach, które bardzo drogo kosztują. Jeśli kupujemy technologie, które kosztują 100 mln zł, to szkolenia po prostu muszą być przeprowadzone tak, aby zachować ciągłość działań tych technologii, aby je prawidłowo wykorzystać. Panie przewodniczący, odpowiedziałem na pytania.

Przewodniczący poseł Michał Jach (PiS):

Dziękuję. Nie słyszę więcej pytań. Jeszcze ktoś? Proszę. Pan poseł Adam Cyrański.

Poseł Adam Cyrański (N):

Rok temu nastąpiła zmiana rządu. Mam pytanie do pana pułkownika, czy nastąpiła również zmiana myślenia. Dlatego, że przez rok obserwujemy karuzelę zmian funkcji na stanowiskach dowódczych. Rozmawiałem kiedyś z panem ministrem. Czy następuje zmiana sposobu myślenia polegająca na tym, że wiemy, że w sektorze cywilnym w Polsce brakuje informatyków? Czy – aby ich w ogóle pozyskać do wojska – nastąpią zmiany w wynagrodzeniach dla tych informatyków? Czy informatycy będą pozyskiwani już w okresie ich kształcenia? Czy będzie im pokazywana ścieżka rozwoju zawodowego? Jest to taka grupa zawodowa, która musi widzieć w tym cel. Trzeba przyjąć, że robią to ze względów patriotycznych, ale są to ludzie, którzy przez cały czas wymagają podniet z tytułu nowych technologii, żeby utrzymać ich na tych stanowiskach.

I moje kolejne pytanie. Czy nastąpi zmiana myślenia? Czy nastąpią zmiany w budżetach? Jeżeli idziemy zwykłą drabinką, która jest właściwie od zarania w strukturach

Ministerstwa Obrony Narodowej, a dodatki są tylko za stanowiska, to w armii nic się nie zmieni. Inne zawody powinny być lepiej wynagradzane. O to mi chodzi, gdyż to może być informacja niejawna. Czy coś dzieje się w tematyce zabezpieczenia danych? Wiadomo z mediów, że Estonia wyrzuciła to wszystko do chmury. Nie ma takich obiektów, które byłyby nas w stanie zabezpieczyć przed impulsem elektromagnetycznym i przed danymi, czy przed gromadzeniem tych danych. Czy robi się coś w kierunku zmiany technologii zabezpieczającej przed elektromagnetycznym atakiem terrorystycznym, który dzisiaj jest dość prosty do wykonania, nawet przy użyciu zwykłych telefonów komórkowych? Dziękuję.

Przewodniczący poseł Michał Jach (PiS):

Czy są jeszcze jakieś pytania? Nie ma. W związku z powyższym proszę o odpowiedzi i przejdziemy do następnego tematu.

Sekretarz stanu w MON Bartosz Kownacki:

Zanim oddam głos panu pułkownikowi, dziękuję za to pytanie, też bardzo cenne, dotyczące zmiany myślenia, czy wydatkowania, jeżeli chodzi o te kwestie. Zastrzegam, że to wydatkowanie na ten sektor, jeżeli chodzi o dodatki, musi być większe. Spojrzałbym na to szerzej, bo to jest w ogóle problem sił zbrojnych. To jest nie tylko kwestia cyberbezpieczeństwa, ale także wielu innych szczególnych specjalizacji. Inspektorat Uzbrojenia, który pozyskuje sprzęt dla całej armii, obraca wieloma miliardami złotych rocznie. Musi być poddawany szczególnej kontroli, ale wynagrodzenie jest tam mniej więcej takie, jak w całych siłach zbrojnych, czy w innych jednostkach sił zbrojnych.

Jest sprawa, która – mam nadzieję – za chwilę będzie też przedmiotem dyskusji, czyli wynagrodzenie dla osób, które przewożą najważniejsze osoby w państwie. Wiemy, jakie są wynagrodzenia dla pilotów w liniach cywilnych. Wiemy, ile taki pilot może uzyskać, a ile może uzyskać nawet przy maksymalnych dodatkach w siłach zbrojnych. Trzeba mieć świadomość, że nigdy nie będzie tak, że administracja publiczna będzie w stanie zaoferować – nieważne, czy to będzie sektor obronności, czy sektor wymiaru sprawiedliwości, czy gospodarki – takich wynagrodzeń, jak sektor prywatny. Ważne jest natomiast, żeby były to wynagrodzenia godne, które ze względu na inne elementy, jak chociażby przywileje emerytalne, stabilność pracy i służby – bo w wojsku bez poczucia misji i służby trudno jest mówić o wykonywaniu swoich zadań – będą rekompensowały tę różnice finansową. Natomiast musimy wiedzieć, że często jest przepaść pomiędzy wynagrodzeniami cywilnymi na rynku informatyków, a tym co zarabiają nawet osoby zajmujące kierownicze stanowiska, czy najwyższe stanowiska w armii. Trzeba mieć tę świadomość, że przy zmianie sposobu myślenia, który następuje i musi następować, te możliwości administracji publicznej na całym świecie są zawsze mniejsze niż rynków prywatnych. Dziękuję.

Szef inspektoratu płk Tomasz Żyto:

Jeżeli mogę, przedstawię informację uzupełniającą. Jeżeli chodzi o dodatkowe wynagrodzenie, bo tu raczej nie chodzi o wynagrodzenie, ale raczej o budowanie takiego kapitału specjalistów, to muszę powiedzieć, że nie wiem, czy minister już ostatecznie podjął taką decyzję. Jednak jeśli chodzi o rozporządzenie w sprawie dodatków widać, że jest próba obecnego kierownictwa, żeby dać dodatki finansowe dla takich grup, jak właśnie kryptologia, czy bezpieczeństwo, więc widać, że ten kierunek jest dobry. Oczywiście, gdybym mógł dzisiaj głosować o rozszerzenie jeszcze tego katalogu do pana ministrze, to również bym to dzisiaj zrobił. Ale ten budżet jest taki, jaki jest, więc myślę, że ten kierunek jest prawidłowy i dobry. W kwestii tego pytania podkreślę też bardzo ważną rzecz.

Patrząc w przyszłość trzeba dzisiaj odnotować, że od dwóch lat widać w miarę intensywne zwiększenie limitów przyjęć do szkół, na edukację, czy na kierunek cyberbezpieczeństwo i kryptologia, który powstał niedawno. W tej chwili mamy ponad stuprocentowe zwiększenie limitu na przyszły rok, z tego, co pamiętam. Jest to taki kierunek, który pozwoli nam zasysać znaczną liczbę ludzi. Jednocześnie te dodatki – mam nadzieję, że na trwałe wejdą do struktury wojskowej – będą potrafiły faktycznie utrzymać te zespoły, bo jednak ta fluktuacja jest spora. To tyle, jeżeli chodzi o dodatki, czy o kwestie środków finansowych, czy w ogóle budowania tych zespołów.

Natomiast, jeżeli chodzi o kwestie tej ochrony, o której pan poseł mówił, to powiem tak. Podkreślałem dzisiaj to, co wielokrotnie przewijało się w mojej wypowiedzi, że resort obrony narodowej generalnie bardzo ostrożnie wchodzi w struktury publiczne. Czyli bazujemy na strukturach wydzielonych. Myślę, że jest to taka dobra bariera do przekroczenia. Oczywiście, korzystamy z tych struktur z zewnątrz i budujemy takie technologie, jakie są na świecie. Niczym się nie różnimy. Czasem mogą one być zbudowane trochę lepiej, trochę głębiej lub w innym miejscu. Jednak generalnie bazujemy na takich samych rozwiązaniach, jak na rynku cywilnym. Myślę, że stosujemy najlepsze praktyki, więc nie ma tu jakiegoś większego, czy mniejszego zagrożenia. Jeżeli będzie jakieś zagrożenie totalne, to będzie ono powodowało faktycznie jakieś perturbacje. Ale trzeba też popatrzeć na to, że ta cała struktura, którą budujemy wewnątrz sił zbrojnych, wykorzystuje nie tylko struktury stacjonarne, ale również mobilne. Nie zawsze potrzebne są struktury stacjonarne, jak jest na rynku cywilnym. A więc mamy te technologie, jeżeli chodzi o komunikację, które nie wymagają struktur stacjonarnych. To tyle, jeżeli chodzi o drugie pytanie pana posła. Panie przewodniczący, dziękuję.

Przewodniczący poseł Michał Jach (PiS):

Dziękuję, panie pułkowniku. Przechodzimy do pkt 2 – informacja ministra obrony narodowej na temat systemu ochrony myśli technologicznej i technologii innowacyjnych na potrzeby pozyskiwanego sprzętu wojskowego dla Sił Zbrojnych Rzeczypospolitej Polskiej. Proszę bardzo, panie ministrze.

Sekretarz stanu w MON Bartosz Kownacki:

Panie przewodniczący, zanim oddam głos panu pułkownikowi Augustynowi, który będzie te kwestie prezentował, oczywiście, od razu deklaruję możliwość, w takim zakresie, jaki będzie, udzielenia odpowiedzi na pytania. Od razu na wstępie chciałbym wskazać, że mamy świadomość wagi tych technologii. W ogóle siły zbrojne generują dużą liczbę technologii innowacyjnych. Dzięki temu ta gałąź gospodarki może się w znakomity sposób rozwijać, co jest przekładane na inne gałęzie gospodarki. Siły zbrojne również muszą zasysać, czy wyszukiwać te technologie innowacyjne, które się pojawiają, które mogą być świetnie wykorzystane na rzecz zwiększenia operacyjności sił zbrojnych i ich potencjału. Dlatego chcielibyśmy tutaj poruszyć raczej kwestie poszukiwania technologii, współpracy przedsiębiorstw podległych Ministerstwu Obrony Narodowej i instytutów naukowo-badawczych w tym zakresie, jak również – bo to jest rzecz bardzo ważna – zarządzania prawami własności intelektualnej z zastrzeżeniem jednej kwestii. Mamy świadomość, że ten proces poszukiwania i zabezpieczenia technologii na rzecz sił zbrojnych dopiero od kilku lat jest traktowany poważnie. Mam nadzieję, że dopiero w perspektywie następnych miesięcy, chociażby poprzez strategiczny przegląd obronny, który również tą kwestią będzie się zajmował, będziemy w stanie wypracować takie procedury, które pozwolą lepiej te technologie identyfikować i zabezpieczać na potrzeby armii.

Dzisiaj jest tak, że chociażby w samym Ministerstwie Obrony Narodowej – mamy tego świadomość, bo jest to konsekwencja ubiegłych lat – Inspektorat Implementacji Innowacyjnych Technologii Obronnych, który reprezentuje tutaj pan pułkownik, ma prawo oceniać technologie, ale nie ma prawa ich nabyć, czy wydatkować pieniędzy na te technologie. To powoduje, że ta struktura jest bardzo rozproszona w siłach zbrojnych, a powinna być skumulowana. Powiem więcej. Przy naszych, jednak mimo wszystko szczupłych możliwościach finansowych, te pieniądze powinny być wydatkowane efektywnie. To znaczy, że jeżeli już identyfikujemy jakieś technologie, to one rzeczywiście muszą być potrzebne siłom zbrojnym. Rzeczywiście muszą mieć zastosowanie w polskim przemyśle. Często te innowacyjne technologie możemy zidentyfikować, a później będą one leżały gdzieś na półce i zupełnie nie będą wykorzystywane dlatego, że nie były nigdy potrzebne, bądź dlatego, że siły zbrojne nie potrafią myśleć perspektywicznie i dostrzec tego, że one mogą być wykorzystane. I to jest taka moja uwaga na wstępie, która podkreśla świadomość tego, że jesteśmy w pewnej procedurze, a Inspektorat, o którym mowa, będzie musiał w perspektywie ulegać pewnym przekształceniom, jeżeli chcemy w taki sposób, jak państwa Europy Zachodniej, wykorzystywać ten potencjał, który drzemie w przemyśle

obronnym, który drzemie w innych sektorach gospodarki, a może być wykorzystywany na potrzeby obronności. Bardzo proszę, panie pułkowniku.

Szef Inspektoratu Implementacji Innowacyjnych Technologii Obronnych płk Sławomir Augustyn:

Dziękuję. Panie ministrze, panie przewodniczący, szanowna Komisjo, chciałbym przedstawić tematykę ochrony myśli technologicznej. Chciałem zaznaczyć, że od sześciu miesięcy jestem szefem i wprowadziłem pewne zmiany. Zdefiniowałem podstawowe elementy, które są związane z pozyskiwaniem innowacyjnych technologii dla obronności i bezpieczeństwa państwa. Pierwsza sprawa – nasza misja. To jest znajdowanie, poszukiwanie i wdrażanie nowych technologii. A więc, ze względu na zdolności operacyjne trzeba pamiętać, że mamy cztery…

Przepraszam, czy mogę wstać? Będzie mi lepiej to tłumaczyć. Dziękuję.

Pamiętajmy o procesie pętli dowodzenia, bo to jest najważniejsze, zresztą nie tylko w biznesie. W ekonomii jest ważność, obserwacja, orientacja, decyzja i działania. Zdefiniowaliśmy w samym Inspektoracie I3TO – to w skrócie Inspektorat Implementacji Innowacyjnych Technologii Obronnych – obserwację satelitarną. Wobec powyższego, razem z Ministerstwem Rozwoju zrobiliśmy strategię sektora kosmicznego i działamy, o czym powiem później, w programach dualnych podwójnego zastosowania dla obronności i bezpieczeństwa, czyli cywilno-wojskowego. Następnie, trzeba pamiętać, że rozpoznanie satelitarne to różne możliwości. Możemy np. wykryć szpiegostwo, ale też przesłać informacje krypto, czyli te informacje, które nie dla wszystkich będą bardzo ważne.

Oprócz tego obserwacja przez platformy, bezzałogowe statki powietrzne, czyli tzw. drony. Ale trzeba pamiętać, że to są bezzałogowe systemy powietrzne, czyli kilka bezzałogowych statków powietrznych, które w odpowiednich warunkach mogą przekazać informacje do centrum operacyjno-eksperckiego – oczywiście – do decyzji stanowiska dowodzenia. Wobec powyższego poszukujemy technologii na tych wszystkich czterech poziomach, czyli obserwacji, orientacji, decyzji i działania. Ponadto jest system szkolenia. Pani poseł powiedziała, że to Akademia Sztuki Wojennej. To prawda. Od września Inspektorat wysyła od nas specjalistów mających wpływ na wymagania operacyjne, które przekształcają się w zdolności operacyjne, na kursy dowódców batalionów dotyczące tego, jaka jest możliwość wdrożenia nowych technologii dla zwiększenia zdolności szybszego wykrycia przeciwnika. Jest to np. m.in. walka radioelektroniczna. Czyli tutaj Inspektorat nie tylko poszukuje, ale implementuje know-how. Czyli wdrażamy wiedzę i przekazujemy ją przyszłym dowódcom, albo dowódcom na poziomie taktycznym i na poziomie operacyjnym.

Ponadto są działania poszukiwania nowoczesnych materiałów i technologii. Co roku mamy taką gale innowacyjności – konkurs, poprzez który poszukujemy nowych technologii. Oprócz tego szukamy sami. Właściwie Inspektorat I3TO stał się częścią wspólną pomiędzy ośrodkami naukowo-badawczymi, a Polską Grupą Zbrojeniową po to, żeby technologie szły w dwie strony. Trzeba pamiętać, że Polska Grupa Zbrojeniowa też ma swoich inżynierów, technologów. Poprzez odpowiednie rozmowy – oczywiście we wszystkich rozmowach zachowana jest poufność – można zwiększyć zdolności np. kołowego transportera opancerzonego „Rosomak". To jest taki przykład. Ale może być też inny, np. samolot. Bezzałogowy statek powietrzny, który ma lepszą optoelektronikę, lepsze możliwości przekazywania i szybciej przekazuje informacje. A informacja, to decyzja. A decyzja, to lepsze maskowanie naszych wojsk, przemiana wojsk w różnym położeniu lub obrona i ochrona. Tak więc tutaj dobra informacja, rzetelna informacja w funkcji czasu jest tutaj bardzo wyraźna i bardzo dobra.

Oczywiście, są działania kryzysowe. Wojsko może również wspierać działania kryzysowe. Robiliśmy i robimy np. tzw. warsztaty polegające na ochronie naszej polskiej linii brzegowej Bałtyku. Będziemy robić góry. Czyli mamy współpracę z gestorami, czyli powiedzmy, że z 21. Brygadą Strzelców Podhalańskich, która ochrania nasze granice. A my pokazujemy te nowe technologie i jak mogą je wykorzystać, żeby nie tylko ochronić nasze życie, ale także życie żołnierzy. Bo musi też być ochrona życia żołnierza. Oczywiście, w obszarze działania mamy elementy powietrzne, lądowe, morskie i wojsk specjal-

nych. Oczywiście, wejdzie tutaj obrona terytorialna, bo ona będzie praktycznie zawierała te wszystkie elementy. Mamy wielką świadomość, że tutaj ten nowy sprzęt dotyczący żołnierza przyszłości, czyli funkcje życiowe żołnierza, czy parametry życiowe, będzie można przekazywać poprzez odpowiedni sygnał do MEDEVAC. Nawet, kiedy żołnierz straci przytomność wiemy, że ma funkcje życiowe i możemy go ratować. Czyli poprawiamy morale żołnierza. Żołnierz wie, że w każdej chwili nawet, gdy zemdleje na polu walki, będzie odebrany.

Obszary działania Inspektoratu. Jednym z nich jest udział w systemie pozyskiwania sprzętu wojskowego. Tu współdziałamy w jednym pionie. Tu Departament Polityki Zbrojeniowej daje nam wytyczne. Z każdego spotkania mamy notatki. One są krótkie, rzetelne i z wnioskami. Wysyłamy je do poszczególnych departamentów, np. do Departamentu Nauki i Szkolnictwa Wojskowego po to, żeby była wymiana tych informacji. Informujemy o każdym spotkaniu innego departamentu. Informujemy ich, czy mamy informacje o danym przemyśle, o danym przedsiębiorcy, czy o danej nauce. Jak to robimy? Pokażą to kolejne slajdy. Szukamy właśnie badań naukowych. Czy to jest np. rozwój technologii kosmicznych? Tak. Próbujemy. Opisaliśmy to.

We wrześniu odbyło się spotkanie zorganizowane przez Inspektorat na terenie Cytadeli, na którym określiliśmy trzy obszary dotyczące obronności i bezpieczeństwa w funkcji sektora kosmicznego. To znaczy, że jest to obserwacja Ziemi, obserwacja kosmosu, czy nie ma np. satelitów szpiegowskich. Jeżeli będziemy mieli naszego satelitę, to będziemy musieli wiedzieć, gdzie jest, kiedy jest w jakim położeniu, bo to jest bardzo ważne. Jak mówiłem, jest to obserwacja Ziemi, ze względu na to, żeby zobaczyć, czy ewentualnie zbliżają się jakieś działania kryzysowe, czy różne czynniki środowiskowe, co da nam możliwość przygotowania na nie społeczeństwa. I tzw. launcher'y, czyli rakiety, które mają je wynieść. Czyli zdefiniowaliśmy trzy obszary, a teraz szukamy środków finansowych. Współpracujemy też z Ministerstwem Rozwoju i z innymi ministerstwami, również z MSWiA po to, żeby te sygnały krypto i to, czego ktoś potrzebuje, było nadzorowane i rzetelnie przedstawiane.

Ochrona technologii krytycznych. Tak. To jest bardzo ważne. Ochrona tych technologii kluczowych. Może nie do końca szybko zbudujemy satelitę, ale jeżeli paliwo będzie nasze, jeżeli zasilanie będzie nasze, bez czego satelita nie poleci, rakieta nie poleci, to nazywamy to technologiami kluczowymi. I szukamy takich technologii, która byłyby polską myślą techniczną, polską nauką, polskim wpływem. Na przykład kodowanie, jest również polską myślą. Chcemy, żeby te kody były w naszych rękach. I to jest bardzo istotne. Co z tego, że będziemy mieli najlepszy sprzęt, jeżeli nie będziemy mieli wpływu na funkcjonowanie tego sprzętu? I tu jest pełna świadomość tego. Pan minister wspomniał, w I3TO jest to robione. Oczywiście, decyzją pana ministra Macierewicza będziemy mieli prawo własności intelektualnej. Ale prace trwają. Wiemy, że w Sejmie też są prace. Chyba dzisiaj też będzie głosowanie dotyczące ustawienia innowacyjności. Żeby skorelować nasze działania z tym prawem, czekamy na tę ustawę.

Wówczas razem będziemy to robić, również poprzez Departament Nauki i Szkolnictwa Wojskowego i Departament Polityki Zbrojeniowej, żeby wspólnie zrobić prawa własności intelektualnej. Chodzi o to, żeby te technologie nie wypływały bez zgody rządzących naszym krajem poza granice Rzeczypospolitej Polskiej. Oczywiście, decyzje zostawiamy tutaj państwu i rządowi. My tu już nie mamy wpływu. Natomiast możemy określić, jakie to są technologie. Kierunki działania. Najważniejszym kierunkiem działania oprócz tego, jest racjonalizatorstwo, które wzięliśmy z Departamentu Nauki i Szkolnictwa Wojskowego. Dlaczego? Dlatego, że to użytkownik, żołnierz może wiedzieć, jak ten sprzęt się sprawuje. Będziemy mieli w resorcie nadzór nad tym. Mało tego. Będziemy wiedzieli, co nie działa właściwie. Możemy dodać innowację i przesłać do danego producenta powiadomienie, że ten sprzęt ma np. niską niezawodność, że uszkadza się, że trzeba w nim to i to poprawić, żeby w kolejnej produkcji zwrócili na to uwagę, żeby ten sprzęt był, może niekoniecznie zmodernizowany, ale ulepszony, na odpowiednim poziomie niezawodności.

Oprócz tego w tej chwili piszemy strategię rozwoju nowych technologii dla zdolności operacyjnych sił zbrojnych na 25-35 lat. Jeszcze dzisiaj nad tym siedzimy. To również

będzie przedstawione panu ministrowi, jakie kluczowe technologie, które wybieraliśmy, mogą spowodować, że poczujemy się bezpiecznie – ale mało tego – że możemy być konkurencyjni na rynku europejskim i światowym. Do powyższego trzeba mieć narzędzia. Mamy bazę danych. Oczywiście, dojścia do tej bazy danych są tylko w naszym resorcie. Do tej bazy wpisujemy codziennie nowe technologie, które próbujemy skorelować, łączyć. Łączymy 2-3 podmioty, które np. wykonują daną technologię. Zaraz pokażę państwu przykład. Pozwala to określić, która technologia może być ważna. Oprócz tego Sztab Generalny lub inny gestor może to sobie znaleźć i uwzględnić w wymaganiach operacyjnych. Oczywiście, jest to jeszcze przesyłane odpowiednimi pismami z wyjaśnieniami, czy można te wymagania uwzględnić w planowaniu w celu zakupu lub czekać w dalszej kolejności na badanie i rozwój danej technologii.

Obecnie Inspektorat ma poziom badań na 6. poziomie, czyli poziom – demonstrator. Chcemy mieć poziom 9, czyli prototyp i możliwość wdrożenia go do produkcji. Czyli chcielibyśmy jeszcze mieć nadzór. W niektórych przypadkach proponujemy tzw. krótką ścieżkę rozwoju po to, żeby dana technologia jak najszybciej, np. za 2-3 lata mogła być ewentualnie uwzględniona w jakiejś produkcji. I tutaj cały czas o tym myślimy. Mamy strategiczny przegląd obronny, w ramach którego odbędą się następne dwie konferencje. Właściwie będą to już warsztaty zamykające, gdzie również będzie opisane to, jak poprzez odpowiednie uwarunkowania prawne skrócić ścieżkę nowych technologii wdrożeniowych do polskiego przemysłu zbrojeniowego.

Przykładowe zidentyfikowane technologie, to są np. perowskity. To nic innego, jak fotowoltaika nadrukowana na folii, która nie tylko poprzez promienie słoneczne, ale również energię może zasilać baterie lub inne urządzenia. Jesteśmy teraz na etapie rozmów, żeby ta technologia została wdrożona. Chcę państwu powiedzieć, że już na początku jest demonstrator. Chcemy zrobić taki pełny prototyp. Nadzorujemy tę technologie, tzn. pozyskaliśmy pieniądze. To jest właśnie problem, że Inspektorat I3TO nie ma w tej chwili bezpośredniego zabezpieczenia finansowego. Możemy rekomendować, chociaż powiem, że te rekomendacje są uwzględniane, w więc nie ma tutaj większego zagrożenia. Natomiast, gdyby była ta szybka ścieżka, to byłaby w resorcie możliwość, żeby ładnie dokonać tej transfuzji, czy przekazania funduszy po to, właśnie ta technologia została jak najszybciej wdrożona.

Kompozyty grafenowe. Oczywiście, grafen nadal jest badany. Jak mi wiadomo, próbuje się dojść do szóstego atomu minimalizacji, co da większą miniaturyzację i dostosowanie do przesyłu energii. Natomiast na razie jesteśmy przy analizie, czy ten grafen w takiej postaci, jak teraz, może być w pełni zastosowany do dalszej produkcji. Następnie mamy energię skierowaną. To bardzo dobra rzecz. Na tę chwilę też są wykonywane projekty. Technologie terahercowe. Właśnie to jest do bezpieczeństwa i ochrony. To jest prześwietlanie np. człowieka w specjalnych bramkach, bez potrzeby zbędnego wyciągania rzeczy osobistych. Mamy urządzenia do walki radioelektronicznej. Trzeba być świadomym, że pierwszy poziom konfliktu, jaki będzie, to będzie uruchomienie walki radioelektronicznej. Jest to walka polegająca na tym, żeby jak najwięcej zaszkodzić przeciwnikowi w sensie łączności. Tutaj na pewno koledzy z Inspektoratu Systemów Informacyjnych to wiedzą, są tego świadomi i robią wszystko, żeby tego uniknąć.

Chcę powiedzieć, że oprócz tego dokonujemy też projektów nadzoru związanych z radarami, optoelektroniką, czyli obserwacją. Oczywiście, to wszystko jest uruchamiane. Myślę, że w przyszłym roku, jeśli będzie możliwość, powinno już być więcej efektów i wdrożeń dlatego, że jest tu 9 poziomów, a każdy poziom trzeba sprawdzić, proszę państwa i nadzorować. Nie możemy sobie na to pozwolić, że przejdziemy do następnego poziomu, a poprzedni nie jest w pełni zrealizowany. Specjaliści z I3TO bardzo skrupulatnie tego pilnują. Oprócz tego mamy udział w programach kosmicznych, jak Galileo, Copernicus, czy oglądanie przestrzeni kosmicznej GovSatcom. Próbujemy wszystko według projektu Horyzont 2020. Jesteśmy członkami międzyresortowego zespołu do spraw polityki kosmicznej w Polsce.

Chcemy też uruchomić te technologie – jak już wcześniej powiedziałem – dualne, czyli podwójnego zastosowania. Jeżeli jest np. chodzik marsjański, badamy, czy dana technologia nie może być wykorzystana również np. w inaczej ukształtowanych terenie

– powiedzmy, górzystym – do systemu rozpoznawczego dla polskiego żołnierza. Tutaj jest projekt systemu ochrony polskiej myśli technicznej. Zaznaczam, że jest to dopiero projekt, który został stworzony. System mógłby w pełni pozwolić na wdrożenie nowych technologii przy jak najmniejszym ryzyku ich niewdrożenia lub znaleźć odpowiedni poziom, tzw. kamień milowy, czyli poziom, na którym coś w tej chwili zatrzymujemy mówiąc, że nie ma sensu dalej iść tą drogą, że trzeba poczekać, aż jakaś inna technologia wspomoże tę pierwotną technologię.

Tutaj najpierw pozyskujemy przez I3TO informacje, które mamy w bazie danych. Oczywiście, są wstępne opinie i analizy gestorów oraz Departamentu Nauki i Szkolnictwa Wojskowego. Jeżeli wstępna analiza jest pozytywna, wówczas, m.in. z Departamentem Polityki Zbrojeniowej i innymi departamentami, np. z Departamentem Prawnym, staramy się uzgodnić, czy jest taka potrzeba, czy to ma sens. Ja nazywam to, że jest to zespół ekspercki. Osoby z różnych dziedzin muszą też o tym wiedzieć. Jeżeli opinia jest pozytywna, wniosek będzie zatwierdzony przez ministra obrony narodowej. Wraz z Departamentem Nauki i Szkolnictwa Wojskowego, albo tzw. szybką ścieżką, czyli pod nadzorem I3TO, będziemy mogli to kontynuować. Może to być finansowane przez Narodowe Centrum Badań i Rozwoju. Oczywiście, wtedy funkcjonuje Departament Nauki i Szkolnictwa Wojskowego. Następuje dopełnienie tego procesu projektowego, a my to nadzorujemy. Zobaczymy, co będzie dalej z tą pozyskiwaną technologią do wdrożenia przez Polską Grupę Zbrojeniową. To jest taki krótki proces pozyskiwania i wdrażania innowacyjnych technologii.

Chcę państwu powiedzieć, że jest to praca bardzo złożona. Tutaj istotny jest nawet dobór osób do I3TO. W ostatnim czasie muszą to być osoby, które już mają nieco szerszą wiedzę, wiedzę analityczną, nie tylko ogólną, ale które potrafią dokonać analizy, syntezy, abstrahowania i wiedzą, jak dokonać odpowiedniego wnioskowania. Dlatego też są tutaj zmiany. Zresztą pan minister też dokonuje różnych zmian. Za zgodą dokonuje się zmian po to, żeby merytorycznie, jakościowo te osoby, które współpracują, mogły rzetelnie i obiektywnie podać daną informację. Na początku jest to bardzo, bardzo istotne. Dziękuję za uwagę. Jeśli są jakieś pytania szanownej Komisji, panie przewodniczący, to proszę.

Przewodniczący poseł Michał Jach (PiS):

Dziękuję, panie pułkowniku. Myślę, że to chyba było przejęzyczenie, że to jest krótki proces. Był to raczej krótki opis złożonego procesu. Czy są jakieś pytania do pana pułkownika? Nie ma. Czy pan minister chce jeszcze zabrać głos? Jeśli nie, to w takim razie wyczerpaliśmy, proszę państwa, te podstawowe tematy.

Natomiast, chcę jeszcze powiedzieć, że właśnie uciekł nam nowy poseł. Chcę państwa poinformować, że mamy nowego kolegę posła. Jest to pan poseł Leszek Ruszczyk z Platformy Obywatelskiej. Był, ale nie doczekał. Chcę poinformować posłów, że na przedsejmowy wtorek, 29 listopada br., zaplanowana została wizytacja Komisji w firmach Doliny Lotniczej – PZL w Mielcu oraz w siedzibie firmy Pratt &Whitney Rzeszów, dawniej WSK. Celem wizytacji będzie zapoznanie się z bieżącym funkcjonowaniem przedsiębiorstw, perspektywami ich rozwoju oraz potencjalnymi projektami możliwymi do realizacji w ramach programu modernizacji technicznej sił zbrojnych. Transport samolotem ma zapewnić Ministerstwo Obrony Narodowej. Wylot z Warszawy ok. godz. 8.30. Myślę, że powrót z Rzeczowa nastąpi ok. godz. 17.00. Ze względów organizacyjno-technicznych bardzo proszę o zgłaszanie deklaracji, co do wzięcia udziału w wizytacji. Koledzy z sekretariatu będą jeszcze do wszystkich państwa dzwonić. Jeżeli nie ma do mnie więcej pytań, to zamykam posiedzenie Komisji. Dziękuję państwu za udział. Do widzenia.